What is claimed is:

1. A method for use in a public-key encryption system, the encryption system having an encryption block encrypting a plaintext m of a length of k_0 to output a ciphertext (α,β) and a decryption block for decrypting the ciphertext (α,β) to provide the plaintext m, comprising the steps of:

(a) choosing variables p, q and g as public-key parameters, wherein p is a large prime number of length k, q is a large prime number dividing $p-1$ and g is a generator for a multiplicative group Z_p^*, wherein $Z_p^* = \{g^0, g^1, g^2, \cdots, g^{q-1}\}$;

(b) choosing and publishing a first hash function H, $H:\{0,\ 1\}^k \rightarrow Z_q$, providing security against an adaptive-chosen-ciphertext-attack and a second hash function G, $G: Z_p^* \rightarrow \{0,\ 1\}^k$, providing security under a computational Diffie-Hellman assumption;

(c) choosing and storing a secret key x satisfying $x \in Z_q$ based on the chosen public-key parameters p, q and g and generating a public key X ($X = g^x$), thereby publishing the public-key parameters p, q and g and the public key X;

(d) encrypting the plaintext m by using the public key X, thereby generating the ciphertext (α,β);

(e) verifying whether the ciphertext (α,β) is valid or not; and

(f) if the ciphertext (α,β) is verified to be valid, decrypting the ciphertext (α,β) by using the secret key x to recover the plaintext m.

2. The method of claim 1, wherein the ciphertext (α,β) is defined as:

$$(\alpha,\beta)=(g^{H(m\|r)}, G(X^{H(m\|r)} \bmod p) \oplus (m\|r))$$

where r is a random string of a length k_1 with $k_0+k_1=k$.

3. The method of claim 2, wherein the verifying step (e) includes the step of (e1) computing $t=G(\alpha^x)\oplus\beta$ and determining whether α of the ciphertext (α,β) is identical to $g^{H(t)}$ or not.

4. The method of claim 3, wherein the decrypting step (f) includes the step of removing the random number r from t to thereby recover the plaintext m.

5. The method of claim 2, wherein the exponentiation operation is replaced by addition operation over elliptic curve group.